REMARKS

Claims 1, 3-18, 20-29 and 31-33 are currently pending in the subject application and are presently under consideration. Claim 27 has been amended herein. A listing of claims and associated status identifiers can be found on pgs. 2-6 of the Reply. Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Rejection of Claims 1, 3-9, 17, 18, 20 and 23 Under 35 U.S.C. §103(a)

Claims 1, 3-9, 17, 18, 20 and 23 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.* ("A secure electronic software distribution (ESD) protocol based on PKC" by Lee *et al.*, EC-Web 2000, LNCS 1875, pp. 63-71, 2000), in view of Hypponen (U.S. 6,986,050 B2), and further in view of Bathrick *et al.* (U.S. 5,825,300). It is respectfully submitted that this rejection should be withdrawn for the following reason. Lee *et al.,* Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

> To reject claims in an application under §103, an examiner must show an unrebutted *prima facie* case of obviousness. A *prima facie* case of obviousness is established by a showing of three basic criteria. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) ***must teach or suggest all the claim limitations.*** *See* MPEP §706.02(j). The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicants' disclosure. *See In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). (emphasis added)

The claimed invention relates to a system and methodology to facilitate secure network communications between remote network entities or parties to a transaction. This is achieved by providing a strong set of security credentials between a master entity such as a service and a remote entity such as a partner. In conjunction with the strong set of security credentials, a protocol is provided that acts as a package, wrapper or container to house the security credentials before delivery from the service to the partner to facilitate secure communications between the parties. In particular, independent claim 1 recites *a wrapper that packages credentials associated with resources of a service;* ***and a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key****, the pass-phrase employed to facilitate access to the credentials, the credentials employed to facilitate access to the resources of the service, and* ***the pass-phrase distributed separately from the credentials.*** Independent claim 18 recites similar limitations. Lee *et al.,* Hypponen and Bathrick *et al.*, individually or in combination, fail to teach or suggest such aspects of the claimed invention.

Lee *et al.* discloses a secure electronic software distribution protocol based on public key cryptography (PKC). When a customer completes a software purchase, a merchant server sends an electronic license to the customer *via* email. When the customer executes an installation program, the program first connects to the authentication agent using a loopback address and predefined port. The authentication agent decrypts using the merchant server's public key and sends the message to the installation program. The installation program then extracts the message, authenticates it and generates a timestamp. However, Lee *et al.* does not disclose or suggest utilizing a pass-phrase to generate a wrapper. On page 3 of the Office Action dated June 29, 2006, the Examiner concedes that Lee *et al.* is silent regarding *a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key, the pass phase distributed separately from the credentials* as taught by independent claims 1 and 18 of applicants' claimed invention.

The Examiner attempts to compensate for the aforementioned deficiencies of Lee *et al.* with Hypponen and Bathrick *et al.* Hypponen discloses a method of securing data stored in an electronic device comprising encrypting the data using a cryptographic key. A user is asked to enter a password and a pass-phrase, the system uses the pass-phrase to generate a cryptographic key, stores it in the system and uses it to encrypt and decrypt the data. A user is allowed entry into the electronic device and the encrypted data by entering the correct pass-phrase. The password is used to authenticate the user at regular intervals while the device is turned on. If the password entered is incorrect, the system asks for the correct pass-phrase to allow entry to the user. In this way, the encrypted data is made inaccessible if a machine is stolen when in a switched on state. Thus, the pass-phrase taught by Hypponen is used to generate a cryptographic key that allows access to encrypted data in a computer device. The pass-phrase is not employed in connection with generation of the cryptographic ***wrapper***. Therefore, Hypponen is silent regarding ***a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key, the pass phase distributed separately from the credentials*** as recited by applicants' subject claims.

Bathrick *et al.* teaches computer security systems and a protected distribution of certificate and keying material between a certification authority and at least one entity in the certification authority's domain. The certifying authority generates keying material, which includes a password and sends it to the subject entity via manual courier or other means that is different from the communication system operating through a network. Once the user receives the keying material, a public and private key pair is generated and the public key is protected using the password. When the user requests the certifying authority for a certificate, he is asked to provide the public key and address for authentication. Nowhere does Bathrick *et al.* teach ***a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key*** as claimed.

In view of the above, it is respectfully submitted that this rejection be withdrawn with respect to independent claims 1 and 18 (which claims 3-9, 17, 20 and 23 depend respectively therefrom).

II. <u>Rejection of Claims 10-12 Under 35 U.S.C. §103(a)</u>

Claims 10-12 are rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.*, in view of Hypponen, in view of Bathrick *et al.*, and further in view of Brainard (SecurSight: An architecture for secure information access, RSA Lab). It is respectfully submitted that this rejection should be withdrawn for the following reasons. Claims 10-12 depend from independent claim 1. As discussed *supra*, Lee *et al.,* Hypponen and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in independent claim 1. Brainard does not make up for the deficiencies of Lee *et al,* Hypponen and Bathrick *et al.* Thus, it is respectfully submitted that this rejection be withdrawn.

III. <u>Rejection of Claims 27-29, 31 and 33 Under 35 U.S.C. §103(a)</u>

Claims 27-29, 31 and 33 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.*, in view of Bathrick *et al.* It is respectfully submitted that this rejection should be withdrawn for the following reason. Lee *et al.*, and Bathrick *et al.*, individually or in combination, do not teach or suggest each and every element set forth in the subject claims.

Independent claims 27, 28, 31 and 33 recite similar limitations, namely, *a second data packet containing* ***a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field.*** Lee *et al.* and Bathrick *et al.* are silent about such novel aspects of applicants' subject claims.

The Examiner concedes that Lee *et al.* fails to disclose a pass-phrase distributed separately from the wrapper field at col. 2, ll. 33-40 and 64-67, but contends that Bathrick *et al.* provides such teaching (*See* Office Action dated June 29, 2006, pg. 10). Applicants' representative respectfully disagrees with such contention.

At the indicated passages, the cited reference discusses the transmission of a password using a manual courier for security. However, the noted password of Bathrick *et al.* is not equivalent to the claimed pass-phrase. The password in the reference is a mechanism to protect transferred data. On the contrary, a pass-phrase generates a wrapper of a password, so that increased security exists through separation of the pass-phrase from the wrapper, where the pass-phrase is needed to access the wrapper. Bathrick *et al.* fails to teach or suggest aspects of the pass-phrase, let alone the separation of a pass-phrase from a wrapper field.

In view of at least the foregoing, it is readily apparent that Lee *et al.* and Bathrick *et al.*, alone or in combination, do not teach or suggest the invention as recited in independent claims 27, 28, 31 and 33 (and associate dependent claim 29). Accordingly, this rejection should be withdrawn.

IV. Rejection of Claims 13-16, 21, 22, 24, 25 and 32 Under 35 U.S.C. §103(a)

Claims 13-16, 21, 22, 24, 25 and 32 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Lee *et al.*, in view of Hypponen, and further in view of Bathrick *et al.* and Brainard. It is respectfully submitted that this rejection should be withdrawn for the following reasons. Lee *et al.*, Hypponen, Bathrick *et al.* and Brainard, individually or in combination, do not teach or suggest each and every element set forth in the subject claims. In particular, claims 13-16 depend from independent claim 1, claims 21, 22, 24 and 25 depend from independent claim 18 and claim 32 depends from independent claim 31. As noted above, Brainard does not make up for the aforementioned deficiencies of Lee *et al.,* Hypponen and Bathrick *et al.* with respect to independent claims 1, 18 and 31. Accordingly, withdrawal of this rejection is requested.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP319US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicants' undersigned representative at the telephone number below.

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/Olivia J. Tsai/______________________
Olivia J. Tsai
Reg. No. 58,350

AMIN, TUROCY & CALVIN, LLP
24TH Floor, National City Center
1900 E. 9TH Street
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731